# BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

## IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.**

JTSB-489-US
IDS

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-178421
(43)Date of publication of application : 30.06.1998

(51)Int.Cl. H04L 9/36
G06F 13/00
H04L 12/66
H04L 12/56

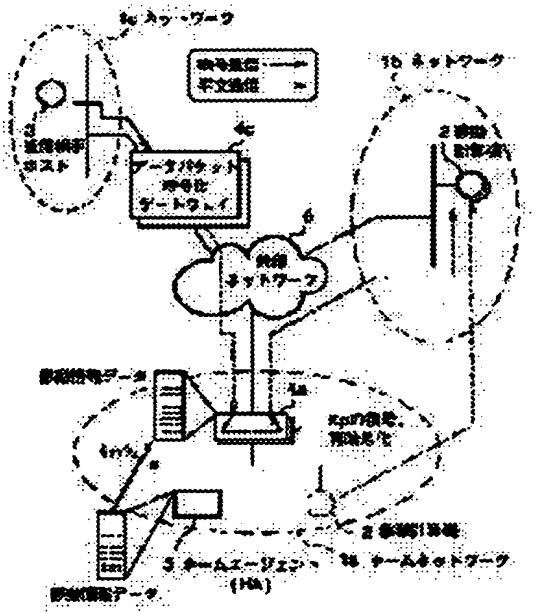
(21)Application number : 09-236045
(22)Date of filing : 01.09.1997

(71)Applicant : TOSHIBA CORP
(72)Inventor : INOUE ATSUSHI
ISHIYAMA MASAHIRO
FUKUMOTO ATSUSHI
TSUDA YOSHIYUKI
SHINPO ATSUSHI
OKAMOTO TOSHIO

(30)Priority
Priority number : 08276186 Priority date : 18.10.1996 Priority country : JP

## (54) PACKET PROCESSOR, MOBILE COMPUTER, PACKET TRANSFERRING METHOD AND PACKET PROCESSING METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To reduce the overhead of packet proc ssing by deciphering/re- ciphering only a packet processing key without processing with respect to the data part of a transferred ciphering packet and the packet to a destination computer.
SOLUTION: Data packet ciphering gate ways 4a and 4c for ciphering communication between a control computers are intalled at networks 1a and 1c. Similarly, a mobile computer 2 is also provided with a packet encoding function similar to the gate ways 4a and 4c. Then, the computer 2 setting inside the network 1a to be a home position moves and cipher-communicates with the communication opposite host 3 of the network 1c. A home agent 5 within the home network 1a is in charge of the position information management and the packet routing of the computer 2 and receives position information from the computer 2. Then a data packet setting a present position to be a transmission destination is transmitted by being capsulated.



LEGAL STATUS
[Date of request for examination] 19.07.2002
[Date of sending the examiner's d cision of rej ction]
[Kind of final disposal of application other than the

(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開番号

特開平10－178421

(43)公開日　平成10年(1998) 6月30日

| (51)Int.Cl.[6] | | 識別記号 | FI | | |
|---|---|---|---|---|---|
| H04L | 9/36 | | H04L | 9/00 | 685 |
| G06F | 13/00 | 351 | G06F | 13/00 | 351E |
| H04L | 12/66 | | H04L | 11/20 | B |
| | 12/56 | | | | 102Z |

審査請求　未請求　請求項の数16　ＯＬ　（全 19 頁）

(21)出願番号　特願平9－236045

(22)出願日　平成９年(1997) ９月１日

(31)優先権主張番号　特願平8－276186

(32)優先日　平８(1996)10月18日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　井上　淳
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(72)発明者　石山　政浩
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(72)発明者　福本　淳
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(74)代理人　弁理士　鈴江　武彦　（外６名）

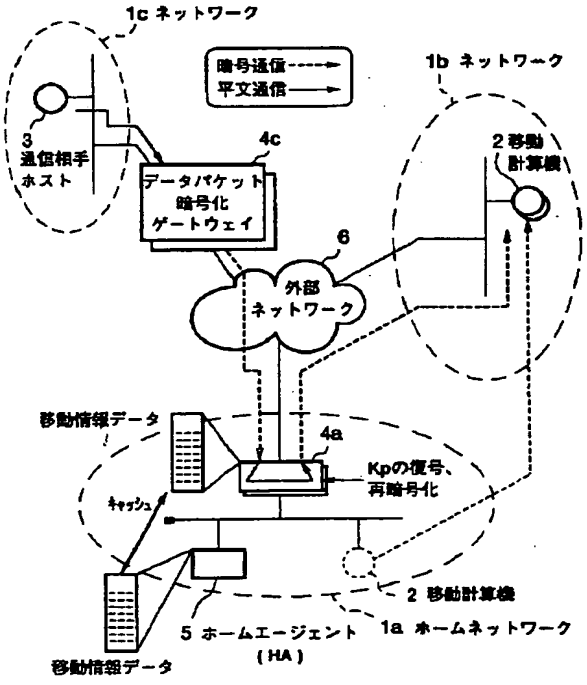
最終頁に続く

(54)【発明の名称】　パケット処理装置、移動計算機装置、パケット転送方法及びパケット処理方法

(57)【要約】

【課題】　暗号化されたパケットを中継するパケット処理装置であって、パケット全体を復号／暗号化することを回避したものを提供すること。

【解決手段】　転送されて来たパケットを受信する手段と、受信されたパケットに対して最後に暗号通信に関する処理を施した装置と自装置との間で共有される第１のマスター鍵で暗号化され前記パケット内にコード化された、パケットのデータ部に対する所定の処理に用いるパケット処理鍵を、該データ部に対する所定の処理は行わずに復号する手段と、このパケットに次に暗号通信に関する処理を施すべき装置と自装置との間で共有される第２のマスター鍵で、復号されたパケット処理鍵を再暗号化して、前記パケット内にコード化する手段と、このパケット処理鍵のコード化がなされたパケットをその宛先へ向けて送信する送信手段とを具備したことを特徴とする。



1

【特許請求の範囲】

【請求項１】暗号化されたパケットを中継するパケット処理装置であって、

転送されて来たパケットを受信する受信手段と、

受信されたパケットに対して最後に暗号通信に関する処理を施した装置と自装置との間で共有される第１のマスター鍵で暗号化され前記パケット内にコード化された、パケットのデータ部に対する所定の処理に用いるパケット処理鍵を、該データ部に対する所定の処理は行わずに復号する復号手段と、

このパケットに次に暗号通信に関する処理を施すべき装置と自装置との間で共有される第２のマスター鍵で、前記復号手段により復号されたパケット処理鍵を再暗号化して、前記パケット内にコード化する再暗号化手段と、

この再暗号化手段によるパケット処理鍵のコード化がなされたパケットをその宛先へ向けて送信する送信手段とを具備したことを特徴とするパケット処理装置。

【請求項２】自装置の管理するネットワーク外の第１の計算機から受信したパケットを、自装置の管理するネットワーク内の所定の位置をホームポジションとし現在該ネットワーク外に移動している第２の計算機へ転送するパケット処理装置であって、

自装置の管理するネットワークをホームポジションとする移動計算機の現在位置の情報を管理し現在該ネットワーク外に移動している該移動計算機宛に転送されてきたパケットを該移動計算機の現在位置に転送する手段を有する移動計算機管理装置と通信する手段と、

前記第１の計算機からのパケットを受信する受信手段と、

受信されたパケットに対して最後に暗号通信に関する処理を施した装置と自装置との間で共有される第１のマスター鍵で暗号化され前記パケット内にコード化された、パケットのデータ部に対する所定の処理に用いるパケット処理鍵を、該データ部に対する所定の処理は行わずに復号する復号手段と、

このパケットに次に暗号通信に関する処理を施すべき装置と自装置との間で共有される第２のマスター鍵で、前記復号手段により復号されたパケット処理鍵を再暗号化して、前記パケット内にコード化する再暗号化手段と、

前記移動計算機管理装置の管理する情報の少なくとも一部を記憶する記憶手段と、

この記憶手段の内容を参照し、前記再暗号化手段によるパケット処理鍵のコード化がなされたパケットを前記第２の計算機へ向けて送信する送信手段とを具備したことを特徴とするパケット処理装置。

【請求項３】自装置の管理するネットワーク内の所定の位置をホームポジションとする移動計算機である第２の計算機が該ネットワーク外に位置することを認識する第１の認識手段と、

前記第２の計算機の通信相手となる前記第１の計算機が

2

自装置の管理するネットワーク外に位置することを認識する第２の認識手段とをさらに具備し、

これら第１及び第２の認識手段により前記第２及び第１の計算機がいずれも自装置の管理するネットワーク外に位置することが認識された場合に前記復号手段、前記再暗号化手段及び前記送信手段を動作させることを特徴とする請求項２に記載のパケット処理装置。

【請求項４】前記送信手段は、前記記憶手段の内容を参照し、前記第２の計算機の現在位置のアドレス宛のパケット内に、前記第２の計算機宛に転送されてきたパケット全体を転送データとしてカプセル化することを特徴とする請求項２に記載のパケット処理装置。

【請求項５】前記第１及び第２の認識手段により前記第２の計算機及び第１の計算機のいずれか一方のみが、自装置の管理するネットワーク内に位置することを認識した場合、パケットがネットワーク外からネットワーク内に入る際にはパケット全体を復号して宛先計算機に向けて送信し、パケットがネットワーク内からネットワーク外に出る際にはパケット全体を暗号化して宛先計算機に向けて送信することを特徴とする請求項２に記載のパケット処理装置。

【請求項６】前記第１及び第２の認識手段は、各ネットワークのパケット処理装置が処理対象とする計算機のリスト情報を参照して、第２の計算機及び第１の計算機の双方が自装置の管理するネットワーク外に位置することを認識することを特徴とする請求項２に記載のパケット処理装置。

【請求項７】前記マスター鍵で暗号化されパケット内にコード化された前記パケット処理鍵をもとに、前記所定の処理においてパケットのデータ部の暗号化または復号に使用するパケット暗号化鍵およびパケットの認証コード生成に使用するパケット認証鍵を生成することを特徴とする請求項１ないし６のいずれか１項に記載のパケット処理装置。

【請求項８】暗号化されたパケットを中継するパケット処理装置のパケット転送方法であって、

転送されて来たパケットを受信し、

受信されたパケットに対して最後に暗号通信に関する処理を施した装置と自装置との間で共有される第１のマスター鍵で暗号化され前記パケット内にコード化された、パケットのデータ部に対する所定の処理に用いるパケット処理鍵を、該データ部に対する所定の処理は行わずに復号し、

このパケットに次に暗号通信に関する処理を施すべき装置と自装置との間で共有される第２のマスター鍵で、復号された前記パケット処理鍵を再暗号化して、前記パケット内にコード化し、

このパケット処理鍵のコード化がなされたパケットをその宛先へ向けて送信することを特徴とするパケット転送方法。

【請求項９】相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機装置であって、
受信したパケットの最外側パケット形式を判別する手段と、
この判別結果に基づいて、カプセル化を解く処理および暗号化パケットを復号する処理を少なくとも含むパケット処理群から実行すべき処理の実行順を決定する手段とを備えたことを特徴とする移動計算機装置。

【請求項１０】相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機装置であって、
受信したパケットの最外側パケット形式を判別する手段と、
この手段により前記最外側パケット形式が移動計算機宛カプセル化形式であると判別された場合は、カプセル化を解く処理を行った後、得られた暗号化パケットを復号する処理を行い、前記最外側パケット形式が暗号化パケット形式であると判別された場合は、暗号化パケットを復号する処理を行った後、得られた移動計算機宛カプセル化パケットのカプセル化を解く処理を行う手段とを備えたことを特徴とする移動計算機装置。

【請求項１１】前記判別する手段はパケットヘッダ内に記述されているパケット形式を示す識別情報に基づいて前記判別を行うことを特徴とする請求項９または１０に記載の移動計算機装置。

【請求項１２】自装置の管理するネットワーク外の第１の計算機から受信したパケットを自組織内の第２の計算機に転送するパケット処理装置であって、
受信したパケットの最外側パケット形式を判別する手段と、
この判別結果に基づいて、カプセル化を解く処理および暗号化パケットを復号する処理を少なくとも含むパケット処理群から実行すべき処理の実行順を決定する手段とを備えたことを特徴とするパケット処理装置。

【請求項１３】自装置の管理するネットワーク外の第１の計算機から受信したパケットを自組織内の第２の計算機に転送するパケット処理装置であって、
受信したパケットの最外側パケットの形式を判別する手段と、
この手段により前記最外側パケット形式が移動計算機宛カプセル化形式であると判別された場合は、カプセル化を解く処理を行った後、得られた暗号化パケットを復号する処理を行い、前記最外側パケット形式が暗号化パケット形式であると判別された場合は、暗号化パケットを復号する処理を行った後、得られた移動計算機宛カプセル化パケットのカプセル化を解く処理を行う手段とを備えたことを特徴とするパケット処理装置。

【請求項１４】自装置の管理するネットワーク外の第１の計算機から受信したパケットを自組織内の第２の計算機に転送するパケット処理装置であって、
受信したパケットの最外側パケットの形式を判別する手段と、



この手段により前記最外側パケット形式が移動計算機宛カプセル化形式であると判別された場合は、カプセル化を解く処理を行って得た暗号化パケットを転送し、前記最外側パケット形式が暗号化パケット形式であると判別された場合は、カプセル化され暗号化されたパケットをそのまま転送する手段とを備えたことを特徴とするパケット処理装置。

【請求項１５】前記判別する手段はパケットヘッダ内に記述されているパケット形式を示す識別情報に基づいて前記判別を行うことを特徴とする請求項１２ないし１４のいずれか１項に記載のパケット処理装置。

【請求項１６】相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機を最終宛先とするパケットに対するノードにおけるパケット処理方法であって、
受信したパケットの最外側パケット形式を判別し、
この判別結果に基づいて、カプセル化を解く処理および暗号化パケットを復号する処理を少なくとも含む処理群から実行すべき処理と実行順を決定することを特徴とするパケット処理方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】移動計算機にパケットを転送するパケット処理装置、相互に接続されたネットワーク間を移動して暗号通信を行うことが可能な移動計算機装置、パケット転送方法及びパケット処理方法に関する。

【０００２】

【従来の技術】計算機システムの小型化、低価格化やネットワーク環境の充実に伴って、計算機システムの利用は急速にかつ種々の分野に広く拡大し、また集中型システムから分散型システムへの移行が進んでいる。特に近年では計算機システム自体の進歩、能力向上に加え、コンピュータ・ネットワーク技術の発達・普及により、オフィス内のファイルやプリンタなどの資源共有のみならず、オフィス外、１組織外とのコミュニケーション（電子メール、電子ニュース、ファイルの転送など）が可能になり、これらが広く利用されはじめた。特に近年では、世界最大のコンピュータネットワーク「インターネット（Ｉｎｔｅｒｎｅｔ）」の利用が普及しており、インターネットと接続し、公開された情報、サービスを利用したり、逆にインターネットを通してアクセスしてくる外部ユーザに対し、情報、サービスを提供することで、新たなコンピュータビジネスが開拓されている。また、インターネット利用に関して、新たな技術開発、展開がなされている。

【０００３】また、このようなネットワークの普及に伴い、移動通信（ｍｏｂｉｌｅ　ｃｏｍｐｕｔｉｎｇ）に対する技術開発も行われている。移動通信では、携帯型の端末、計算機を持ったユーザがネットワーク上を移動

して通信する。ときには通信を行いながらネットワーク上の位置を変えていく場合もあり、そのような通信において変化する移動計算機のネットワーク上のアドレスを管理し、正しく通信内容を到達させるための方式が必要である。

【０００４】また、ネットワークが普及し、ネット間の自由な接続が実現され、膨大なデータ、サービスのやりとりがなされる場合、セキュリティ上の問題を考慮する必要が生じてくる。例えば、組織内部の秘密情報の外部ネットワークへの漏洩をいかに防ぐか、という問題や、組織外からの不正な侵入から、組織内ネットワークに接続された資源、情報をいかに守るか、という問題である。インターネットは、当初学術研究を目的に構築されたため、ネットワークの接続による自由なデータサービスのやりとりを重視しており、このようなセキュリティ上の問題は考慮されていなかったが、近年多くの企業、団体がインターネットに接続するようになり、セキュリティ上の問題から自組織ネットワークを防衛する機構が必要となってきた。

【０００５】そこで、インターネット上でデータパケットを交換する際に、外部にデータパケットを送出する前にその内容を暗号化し認証コードをつけ、受信したサイトで認証コードを確認し復号化する、という方法がある。この方法によれば、たとえ組織外のユーザが外部ネットワーク上のデータパケットを取り出しても、内容が暗号化されているので、決してその内容が漏洩することがなく、安全な通信が確保できる。

【０００６】このような暗号化通信をサポートするゲートウェイ計算機で守られた（ガードされた）ネットワーク同士であれば相互に暗号化通信が可能であり、また前述の移動計算機が自分でパケットの暗号化、復号を行う機能をサポートしていれば、任意のゲートウェイ間、またはゲートウェイ～移動計算機間で暗号化通信がサポートできる。例えば、図１５では、元々ホームネットワーク１ａに属していた移動計算機２が、他のネットワーク１ｂに移動し、ネットワーク１ｃ内の他の計算機（ＣＨ）３と暗号化、復号機能をサポートするゲートウェイ４ａ，４ｃを介して暗号通信を行う。

【０００７】一般に移動通信を行う場合、移動計算機の移動先データを管理するルータ（ホームエージェント）を置き、移動計算機宛データの送信はそのホームエージェントを経由することで、移動計算機に対するデータの経路制御を行う。図１５では、ホームエージェント（ＨＡ）５がこの役割を行う。

【０００８】パケットの転送経路は、通信相手３→ゲートウェイ４ｃ→ゲートウェイ４ａ→ホームエージェント５→ゲートウェイ４ａ→移動計算機２となる。もしネットワーク１ｂのゲートウェイで復号を行う場合には、通信相手３→ゲートウェイ４ｃ→ゲートウェイ４ａ→ホームエージェント５→ゲートウェイ４ａ→ネットワーク１ｂのゲートウェイ→移動計算機２となる。



【０００９】いずれの場合にも、ゲートウェイ４ａにて一旦パケットは復号され、ホームエージェント５との間を往復した後、ゲートウェイ４ａにて暗号化される。つまり、ゲートウェイ４ａでは、パケット全体（パケットのデータ部）を２回も暗号処理していることになる。

【００１０】一般に、データパケットの暗号化、復号は非常に計算量の大きい処理であり、上記のパケットシーケンスは非常に冗長である。特に、多数の移動計算機を同時にサポートする場合、システム全体のスループットを著しく低下させかねない。

【００１１】また、暗号化されたパケットを中継するルータなどの装置でも、受信したパケットを復号し暗号化して中継する場合、同様の問題点があった。一方、移動計算機へのカプセル化によるパケット転送とパケット暗号化によるセキュリティ対応を行うシステムにおいて、システム構成要素間の位置関係等により、パケットに対する移動処理および暗号化処理が任意の順序で行われる場合、パケットを受信する移動計算機では、もとの内容を正しく復元することができなかった。

【００１２】また、移動計算機へのカプセル化によるパケット転送とパケット暗号化によるセキュリティ対応を行うシステムにおいて、システム構成要素間の位置関係等により、パケットに対する移動処理および暗号化処理が任意の順序で行われる場合、パケットを受信する移動計算機側にあってパケットを移動計算機に転送するパケット処理装置では、正しくパケットを転送する処理を行うことができなかった。

【００１３】

【発明が解決しようとする課題】移動通信においては、移動中の計算機宛のパケットについては、移動計算機の移動先データを管理するホストを経由して転送を行う。その際、移動計算機が通信相手とパケットの暗号化、復号を伴う通信を、各ネットワークのゲートウェイにより行う場合、移動中の移動計算機宛のデータパケットは、ホームネットワークの暗号化ゲートウェイで一旦復号されてホームエージェントに到達し、移動計算機の現在位置が検索されてホームエージェントから発信され、再度ホームネットワークの暗号化ゲートウェイで暗号化されてから移動計算機に向けて送り出される。したがって、ホームネットワークの暗号化ゲートウェイでは、計算量の大きい、復号、暗号化を２度行うことになり、冗長であり、またシステム全体のボトルネックの原因となる危険があった。また、暗号化されたパケットを中継するルータなどの装置でも、受信したパケットを復号し暗号化して中継する場合、同様の問題点があった。

【００１４】一方、移動計算機へのカプセル化によるパケット転送と、パケット暗号化によるセキュリティ対応を行うシステムにおいて、システム構成要素間の位置関係等により、パケットに対する移動処理および暗号化処

理が任意の順序で行われる場合、パケットを受信する移動計算機側やパケットを転送するパケット処理装置側では、正しくパケット処理を行うことができなかった。

【００１５】本発明は、上記事情を考慮してなされたもので、暗号化されたパケットを中継するパケット処理装置において、パケット全体を復号、再暗号化することを回避して、オーバーヘッドを削減することができるパケット処理装置及びパケット転送方法を提供することを目的とする。

【００１６】また、本発明は、移動中の移動計算機を宛先とするパケットについては移動計算機の位置情報を管理するホームエージェントを介して暗号化通信が行われ、また移動計算機宛の暗号化パケットをホームネットワークのパケット処理装置で処理する通信システムにおいて、ホームネットワークのパケット処理装置が移動中の移動計算機を宛先とするパケットについてパケット全体を復号、再暗号化することを回避して、オーバーヘッドを削減することができるパケット処理装置及びパケット転送方法を提供することを目的とする。

【００１７】また、本発明は、移動計算機に対する移動箇所アドレスのカプセル化処理と暗号化の処理が任意の順序で実行されても正しく内容を復元できる移動計算機装置及びパケット処理方法を提供することを目的とする。

【００１８】また、本発明は、移動計算機に対する移動箇所アドレスのカプセル化処理と暗号化の処理が任意の順序で実行されても正しくパケットを移動計算機に転送できるパケット処理装置及びパケット処理方法を提供することを目的とする。

【００１９】

【課題を解決するための手段】本発明（請求項１）は、暗号化されたパケットを中継するパケット処理装置（例えば、データパケット暗号化ゲートウェイ、セキュリティルータ）であって、転送されて来たパケットを受信する受信手段と、受信されたパケットに対して最後に暗号通信に関する処理を施した装置と自装置との間で共有される第１のマスター鍵で暗号化され前記パケット内にコード化された、パケットのデータ部に対する所定の処理に用いるパケット処理鍵を、該データ部に対する所定の処理は行わずに復号する復号手段と、このパケットに次に暗号通信に関する処理を施すべき装置と自装置との間で共有される第２のマスター鍵で、前記復号手段により復号されたパケット処理鍵を再暗号化して、前記パケット内にコード化する再暗号化手段と、この再暗号化手段によるパケット処理鍵のコード化がなされたパケットをその宛先へ向けて送信する送信手段とを具備したことを特徴とする。

【００２０】本発明によれば、転送されてきた暗号化パケットのデータ部に対する所定の処理は行わずに、パケット処理鍵のみ復号・再暗号化して宛先計算機へ向けて転送することにより、全てのパケットについてデータ部に対する所定の処理を行う従来技術と比べ、パケット処理のオーバーヘッドを低減することができる。



【００２１】なお、次段のパケット処理装置がパケットのデータ部に対する所定の処理を行えない場合には、自装置にて該所定の処理を行ってから次段へ転送する。本発明は、このようなケースをも包含するものである。

【００２２】本発明（請求項２）は、自装置の管理するネットワーク外の第１の計算機から受信したパケットを、自装置の管理するネットワーク内の所定の位置をホームポジションとし現在該ネットワーク外に移動している第２の計算機へ転送するパケット処理装置であって、自装置の管理するネットワークをホームポジションとする移動計算機の現在位置の情報を管理し現在該ネットワーク外に移動している該移動計算機宛に転送されてきたパケットを該移動計算機の現在位置に転送する手段を有する移動計算機管理装置（例えば、ホームエージェント）と通信する手段と、前記第１の計算機からのパケットを受信する受信手段と、受信されたパケットに対して最後に暗号通信に関する処理を施した装置（第１の計算機、この第１の計算機を管理するパケット処理装置、または経路途中の暗号通信に関する処理機能を持つルータ装置）と自装置との間で共有される第１のマスター鍵で暗号化され前記パケット内にコード化された、パケットのデータ部に対する所定の処理に用いるパケット処理鍵を、該データ部に対する所定の処理は行わずに復号する復号手段と、このパケットに次に暗号通信に関する処理を施すべき装置（第２の計算機、この第２の計算機を管理するパケット処理装置、または経路途中の暗号通信に関する処理機能を持つルータ装置）と自装置との間で共有される第２のマスター鍵で、前記復号手段により復号されたパケット処理鍵を再暗号化して、前記パケット内にコード化する再暗号化手段と、前記移動計算機管理装置の管理する情報の少なくとも一部を記憶する記憶手段と、この記憶手段の内容を参照し、前記再暗号化手段によるパケット処理鍵のコード化がなされたパケットを前記第２の計算機へ向けて送信する送信手段とを具備したことを特徴とする。

【００２３】前記記憶手段には、予め前記移動計算機管理装置の管理する情報の少なくとも一部をキャッシュするようにしても良いし、必要時に情報を得て格納するようにしても良い。

【００２４】本発明によれば、自装置の管理するネットワーク内の計算機宛のパケットであれば、復号手段で得られたパケット処理鍵を用いて、パケットのデータ部に対して所定の処理を行ってから、該ネットワーク内の計算機へ転送するが、自装置の管理するネットワーク外の計算機宛のパケットであれば、パケット処理鍵のみ復号・再暗号化して宛先計算機へ向けて転送することにより、全てのパケットについてデータ部に対する所定の処

理を行う従来技術と比べ、パケット処理のオーバーヘッドを低減することができる。なお、自装置の管理するネットワーク外の計算機宛のパケットであっても、次段のパケット処理装置がパケットのデータ部に対する所定の処理を行えない場合には、自装置にて該所定の処理を行ってから次段へ転送する。本発明は、このようなケースをも包含するものである。

【００２５】好ましくは、自装置の管理するネットワーク内の所定の位置をホームポジションとする移動計算機である第２の計算機が該ネットワーク外に位置することを認識する第１の認識手段と、前記第２の計算機の通信相手となる前記第１の計算機が自装置の管理するネットワーク外に位置することを認識する第２の認識手段とをさらに具備し、これら第１及び第２の認識手段により前記第２及び第１の計算機がいずれも自装置の管理するネットワーク外に位置することが認識された場合に前記復号手段、前記再暗号化手段及び前記送信手段を動作させるようにしても良い。

【００２６】好ましくは、前記送信手段は、前記記憶手段の内容を参照し、前記第２の計算機の現在位置のアドレス宛のパケット内に、前記第２の計算機宛に転送されてきたパケット全体を転送データとしてカプセル化するようにしても良い。

【００２７】好ましくは、前記第１及び第２の認識手段により前記第２の計算機及び第１の計算機のいずれか一方のみが、自装置の管理するネットワーク内に位置することを認識した場合、パケットがネットワーク外からネットワーク内に入る際にはパケット全体を復号して宛先計算機に向けて送信し、パケットがネットワーク内からネットワーク外に出る際にはパケット全体を暗号化して宛先計算機に向けて送信するようにしても良い。

【００２８】好ましくは、前記第１及び第２の認識手段は、各ネットワークのパケット処理装置が処理対象とする計算機のリスト情報を参照して、第２の計算機及び第１の計算機の双方が自装置の管理するネットワーク外に位置することを認識するようにしても良い。

【００２９】好ましくは、前記マスター鍵で暗号化されパケット内にコード化された前記パケット処理鍵をもとに、前記所定の処理においてパケットのデータ部の暗号化または復号に使用するパケット暗号化鍵およびパケットの認証コード生成に使用するパケット認証鍵を生成するようにしても良い。

【００３０】本発明（請求項８）は、暗号化されたパケットを中継するパケット処理装置のパケット転送方法であって、転送されて来たパケットを受信し、受信されたパケットに対して最後に暗号通信に関する処理を施した装置と自装置との間で共有される第１のマスター鍵で暗号化され前記パケット内にコード化された、パケットのデータ部に対する所定の処理に用いるパケット処理鍵を、該データ部に対する所定の処理は行わずに復号し、



このパケットに次に暗号通信に関する処理を施すべき装置と自装置との間で共有される第２のマスター鍵で、復号された前記パケット処理鍵を再暗号化して、前記パケット内にコード化し、このパケット処理鍵のコード化がなされたパケットをその宛先へ向けて送信することを特徴とする。

【００３１】本発明（請求項９）は、相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機装置であって、受信したパケットの最外側パケット形式を判別する手段と、この判別結果に基づいて、カプセル化を解く処理および暗号化パケットを復号する処理を少なくとも含むパケット処理群から実行すべき処理の実行順を決定する手段とを備えたことを特徴とする。

【００３２】本発明（請求項１０）は、相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機装置であって、受信したパケットの最外側パケット形式を判別する手段と、この手段により前記最外側パケット形式が移動計算機宛カプセル化形式であると判別された場合は、カプセル化を解く処理を行った後、得られた暗号化パケットを復号する処理を行い、前記最外側パケット形式が暗号化パケット形式であると判別された場合は、暗号化パケットを復号する処理を行った後、得られた移動計算機宛カプセル化パケットのカプセル化を解く処理を行う手段とを備えたことを特徴とする。

【００３３】好ましくは、前記判別する手段はパケットヘッダ内に記述されているパケット形式を示す識別情報に基づいて前記判別を行うようにしてもよい。本発明（請求項１２）は、自装置の管理するネットワーク外の第１の計算機から受信したパケットを自組織内の第２の計算機に転送するパケット処理装置（例えば、フォーリンエージェント、フォーリンエージェント機能を持つデータパケット暗号化ゲートウェイ）であって、受信したパケットの最外側パケット形式を判別する手段と、この判別結果に基づいて、カプセル化を解く処理および暗号化パケットを復号する処理を少なくとも含むパケット処理群から実行すべき処理の実行順を決定する手段とを備えたことを特徴とする。

【００３４】本発明（請求項１３）は、自装置の管理するネットワーク外の第１の計算機から受信したパケットを自組織内の第２の計算機に転送するパケット処理装置（例えば、フォーリンエージェント、フォーリンエージェント機能を持つデータパケット暗号化ゲートウェイ）であって、受信したパケットの最外側パケットの形式を判別する手段と、この手段により前記最外側パケット形式が移動計算機宛カプセル化形式であると判別された場合は、カプセル化を解く処理を行った後、得られた暗号化パケットを復号する処理を行い、前記最外側パケット形式が暗号化パケット形式であると判別された場合は、暗号化パケットを復号する処理を行った後、得られた移動計算機宛カプセル化パケットのカプセル化を解く処理

を行う手段とを備えたことを特徴とする。

【００３５】本発明（請求項１４）は、自装置の管理するネットワーク外の第１の計算機から受信したパケットを自組織内の第２の計算機に転送するパケット処理装置（例えば、フォーリンエージェント、フォーリンエージェント機能を持つデータパケット暗号化ゲートウェイ）であって、受信したパケットの最外側パケットの形式を判別する手段と、この手段により前記最外側パケット形式が移動計算機宛カプセル化形式であると判別された場合は、カプセル化を解く処理を行って得た暗号化パケットを転送し、前記最外側パケット形式が暗号化パケット形式であると判別された場合は、カプセル化され暗号化されたパケットをそのまま転送する手段とを備えたことを特徴とする。

【００３６】好ましくは、前記判別する手段はパケットヘッダ内に記述されているパケット形式を示す識別情報に基づいて前記判別を行うようにしてもよい。本発明（請求項１６）は、相互に接続されたネットワーク間を移動して通信を行うことが可能な移動計算機を最終宛先とするパケットに対するノード（例えば、移動計算機、フォーリンエージェント、フォーリンエージェント機能を持つデータパケット暗号化ゲートウェイ）におけるパケット処理方法であって、受信したパケットの最外側パケット形式を判別し、この判別結果に基づいて、カプセル化を解く処理および暗号化パケットを復号する処理を少なくとも含む処理群から実行すべき処理と実行順を決定することを特徴とする。

【００３７】なお、以上の装置に係る発明は方法に係る発明としても成立する。また、上記の発明は、相当する手順あるいは手段をコンピュータに実行させるためのプログラムを記録した機械読取り可能な媒体としても成立する。

【００３８】

【発明の実施の形態】以下、図面を参照しながら発明の実施の形態を説明する。

（第１の実施の形態）図１に、本発明の一実施形態に係るネットワークの基本構成を示す。

【００３９】本実施形態では、ホームネットワーク１ａ、外部のネットワーク１ｂ，１ｃがインターネット６を介して相互に接続されている場合について説明する。ネットワーク１ａ，１ｃには、それらが管理する計算機間で暗号化通信を行うためのデータパケット暗号化ゲートウェイ４ａ，４ｃが設置されている。また、本実施形態では、移動計算機２もデータパケット暗号化ゲートウェイ４ａ，４ｃと同様のパケット暗号化機能を持つものとする。これらデータパケット暗号化ゲートウェイ４ａ，４ｃや移動計算機２の間で暗号化通信が行われる。

【００４０】ここでは、ネットワーク１ａ内の所定の位置をホームポジションとする移動計算機２は、移動の結果ネットワーク１ｂにあるものとする。また、移動計算機２が暗号化通信をする通信相手ホスト３は、ネットワーク１ｃにあるものとする。



【００４１】移動計算機２の位置情報の管理、移動計算機２宛のパケットのルーティングを司るのが、ホームネットワーク１ａ内のホームエージェント（ＨＡ）５である。移動計算機２がホームネットワーク１ａを離れ移動先に行くと、その位置情報（必要に応じてさらに位置情報の有効期限など）を含む登録メッセージをホームエージェント５に送る。

【００４２】ホームエージェント５は、この情報をもとに、移動計算機２宛のパケットがホームネットワーク１ａに到達したら、これを受け取って、パケット全体を、移動情報に示される現在位置を送信先とするデータパケットに整形（カプセル化）して、送信する。移動計算機２は、このデータを受け取るとカプセル化を解いて所定のデータを受信する。

【００４３】なお、ホームネット１ａ内には、暗号通信に関する処理を行わないルータを介してサブネットワークが階層的に接続される場合もあるが、この場合には各サブネットワークごとにホームエージェントが設けられるものとする。そして、移動計算機がホームの位置から、暗号通信に関する処理を行わないルータを介した他のサブネットワークに移動した場合、この計算機はホームネット外に移動したものには該当しないものとして扱うことができる。

【００４４】また、ホームネット１ａには、データパケット暗号化ゲートウェイを介してサブネットワークが階層的に接続される場合もある。移動計算機がホームの位置から、データパケット暗号化ゲートウェイを介した他のサブネットワークに移動した場合、この計算機はホームネット１ａ外に移動したものに該当するものとして扱うことができる。

【００４５】ところで、この移動通信の規約にしたがって通信を行うと、前述したように従来は図８のように、データパケット暗号化ゲートウェイ４ｃと４ａの間で暗号通信が行われ、データパケット暗号化ゲートウェイ４ａで暗号化されたデータ部分を復号されたパケットがホームエージェント５に到達し、カプセル化されて再度ゲートウェイ４ａで暗号化される。そして、ゲートウェイ４ａと移動計算機２の間で再度暗号通信を行うことになる。すなわち、ゲートウェイ４ａではパケットのデータ部に対して処理コストの大きい２度の処理、すなわち暗号化と復号を行っている。

【００４６】これに対して本実施形態では、以下のようにして、データパケット暗号化ゲートウェイ４ａでの復号と再暗号化の処理コストを大幅に削減する。以下、本実施形態について、暗号化通信を行うパケット形式とデータパケット暗号化ゲートウェイ４ａでの処理を中心に説明する。

【００４７】まず、図２に暗号化通信を行うパケット形

式の一例を示す。図２において、パケットは、通常のＩＰパケットヘッダの後に、鍵情報ヘッダ、認証ヘッダ、暗号化ヘッダが続き、その後に暗号化されたデータ部が続く。

【００４８】ＩＰヘッダには、暗号化を行った装置のアドレスと復号を行うべき装置のアドレスが含まれる。鍵情報ヘッダには、鍵暗号化のアルゴリズム、パケット暗号化のアルゴリズム、認証のアルゴリズムの指定情報に加え、パケット処理鍵Ｋｐを２つのデータパケット暗号化ゲートウェイ間（あるいはデータパケット暗号化ゲートウェイと移動計算機との間）で共有されるマスター鍵Ｋｉｊで暗号化したものをエンコードしてある。パケット処理鍵Ｋｐは送り手の側でランダムに生成される鍵で、これをもとにパケット認証鍵Ａ＿Ｋｐやパケット暗号鍵Ｅ＿Ｋｐが計算される。なお、マスター鍵を時間情報（カウンタｎ）の関数Ｋｉｊｎとしても良い。

【００４９】なお、２つのデータパケット暗号化装置間あるいはデータパケット暗号化装置と移動計算機の間で共有されるマスター鍵は、例えば、秘密鍵の交換や、公開鍵と秘密鍵による導出（例えば、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ法）により生成することができる。

【００５０】次に、ゲートウェイ４ａにおいて、パケット処理鍵Ｋｐ部分のみの復号、再暗号化ができるのは、移動計算機２とその通信相手３の双方がホームネット１ａ外にいる場合である。例えば、図４のように通信相手３がホームネット１ａ内にいる場合や、図５のように移動計算機２がホームネット１ａ内にいる場合では、一方の通信が暗号化にならず、ホームエージェント５を通過しなくてはいけない（図４や図５ではゲートウェイ４ａにおいてパケットのデータ部に対する暗号化等が行われる）。

【００５１】したがって、本実施形態のパケット処理鍵Ｋｐの復号、再暗号化、およびホームエージェント５に代わっての経路制御を暗号化ゲートウェイ４ａで行うためには、移動計算機２、その通信相手３の双方がホームネットワーク外にあることを認識することが必要になる。

【００５２】このため、本実施形態では、暗号化ゲートウェイ４ａに、移動計算機２がホームネットワーク１ａ外に位置するか否か、および通信相手となる計算機３がホームネットワーク１ａ外に位置するか否かをそれぞれ認識する計算機位置認識部（図示せず）を設ける。例えば、通信システム内のいずれかの場所（分散していても良い）に、各ゲートウェイがどの計算機に対するパケットを処理対象とするかを示す情報のデータベース（具体例としては各ゲートウェイのネットワークアドレスと、その処理対象となる計算機群のネットワークアドレスの対応情報）を管理するサーバ装置を設置し、あるいはゲートウェイが存在する各ネットワーク内で、そのゲートウェイがどの計算機に対するパケットを処理対象とするかを示す情報のデータベースを保持し、ゲートウェイが該データベースを検索することにより実現できる。



【００５３】次に、本実施形態では、ホームネットワーク１ａのデータパケット暗号化ゲートウェイ４ａでのパケット処理鍵Ｋｐの復号、およびデータパケット暗号化ゲートウェイ４ａ～移動計算機２間でのマスター鍵での再暗号化に加え、本来ホームエージェント５で行われる移動計算機２に対するデータのカプセル化処理も行うようにしている。このため、ホームエージェント５に保持されている移動情報データをデータパケット暗号化ゲートウェイ４ａにコピーしキャッシュ情報として保持する。例えば、移動計算機の登録メッセージを処理する際に、その登録内容をデータパケット暗号化ゲートウェイ４ａ内の記憶手段に格納することで実現できる。

【００５４】なお、ホームエージェント５に保持されている移動情報データをデータパケット暗号化ゲートウェイ４ａにキャッシュする代わりに、必要なときにデータパケット暗号化ゲートウェイ４ａがホームエージェント５から情報を取得しても良い。

【００５５】次に、図３に各ノードでのパケット処理の流れを概念的に示す。まず、移動計算機２の通信相手となる計算機３から、該移動計算機３がそのホームネットワーク１ａにいるものとしてＩＰパケットが生成されて送り出される。

【００５６】通信相手ホスト３から移動計算機２に宛てて出されたパケットは、ゲートウェイ４ｃにおいて、パケットのデータ部が暗号化され、またゲートウェイ４ａ～４ｃ間のマスター鍵でパケット処理鍵Ｋｐが暗号化され、また認証データが付加されるなどして、送り出される。

【００５７】ホームネットワーク１ａのデータパケット暗号化ゲートウェイ４ａでは、移動計算機２のホームアドレス宛のデータを受け取ると、ゲートウェイ４ａ～４ｃ間のマスター鍵で暗号化されているパケット処理鍵Ｋｐを復号し、ゲートウェイ４ａ～移動計算機２間のマスター鍵で再度暗号化する。さらに、キャッシュされた移動情報を使い、移動計算機２の現在位置アドレスをヘッダとしてデータグラムをカプセル化して送信する。

【００５８】このようにして移動計算機２にパケットが到達すると、移動計算機２では、カプセル化を解き、パケット処理鍵Ｋｐを復号してパケット認証鍵やパケット暗号鍵を求め、さらに認証コードの確認、データ部の復号を行って、転送データを取得することができる。

【００５９】なお、前述したように、図４のように通信相手３がホームネット１ａ内にいる場合は、データパケット暗号化ゲートウェイ４ａでは、パケットのデータ部の暗号化、認証データの付加、パケット処理鍵の暗号化が行われる。

【００６０】また、図５のように移動計算機２がホームネット１ａ内にいる場合は、データパケット暗号化ゲー

トウェイ４ａでは、パケット処理鍵の復号、認証データの確認、パケットのデータ部の復号が行われる。また、移動計算機２がホームの位置から、暗号通信に関する処理を行わないルータを介した他のサブネットワークに移動した場合、図５のようにパケット暗号化ゲートウェイ４ａからホームエージェント５を介して計算機２にＩＰパケットが転送される。移動計算機２がホームの位置にいる場合、パケット暗号化ゲートウェイ４ａから直接、計算機２にＩＰパケットが転送される。

【００６１】さて、前述したように、従来は暗号化を伴う移動通信においては、移動計算機宛のデータパケットを、ホームエージェント経由でルーティングするためにホームネットワークのゲートウェイで復号、暗号化を２度行う必要があった。

【００６２】これに対して本実施形態によれば、ホームネットワークのゲートウェイ上にホームエージェントの移動位置管理情報のキャッシュを保持するなどして、移動計算機の経路制御をホームネットワークのゲートウェイ上で行い、またデータパケットのパケット処理鍵を暗号化してパケット内にエンコードすることにより、パケット処理鍵のみを復号、再暗号化するだけで、ホームエージェント発のパケットを再構成することで、データパケット全体の復号、暗号化処理を回避して、パケット処理のオーバーヘッドを最小化することができる。

【００６３】なお、本実施形態では、移動計算機２で最後の復号を行ったが、その代わりに、移動先ネットワーク１ｂに存在する暗号化ゲートウェイで復号等を行う場合にも、本発明は適用可能である。

【００６４】次に、ある一纏まりのネットワークが階層構造を持つ場合について説明する。図６に、階層構造を持つネットワークの一例を示す。図６では、データパケット暗号化ゲートウェイ４ａに直接接続されたバス２１に、さらに暗号通信に関する処理機能を持つデータパケット暗号化ゲートウェイ４ｅを介してバス２２が接続され、また暗号通信に関する処理機能を持たないルータ１４ｆを介してバス２３が接続され、サブネットワークが階層構造を形成している。

【００６５】この場合、データパケット暗号化ゲートウェイ４ａは、サブネットワークＡ，Ｃを管理対象とし、データパケット暗号化ゲートウェイ４ｅは、サブネットワークＢを管理対象とする。

【００６６】このような構成において、サブネットワークＡをホームポジションとする計算機２が、サブネットワークＢ内に移動した場合、データパケット暗号化ゲートウェイ４.ａは、計算機２が自装置の管理するネットワーク外に移動したものと認識する。したがって、データパケット暗号化ゲートウェイ４ａは、この計算機２と外部ネットワークを介したネットワーク１ｃ（図１参照）にいる計算機との間で通信されるパケットを転送する場合、図１の場合と同様に、外部ネットワーク側から移動



計算機２のホームアドレス宛のデータを受け取ると、ゲートウェイ４ａ～４ｃ間のマスター鍵で暗号化されているパケット処理鍵Ｋｐを復号し、ゲートウェイ４ａ～ゲートウェイ４ｅ間のマスター鍵で再度暗号化する。さらに、キャッシュされた移動情報を使い、移動計算機２の現在位置アドレスをヘッダとしてデータグラムをカプセル化して送信する。

【００６７】一方、サブネットワークＡをホームポジションとする計算機２が、サブネットワークＣ内に移動した場合、データパケット暗号化ゲートウェイ４ａは、計算機２が自装置の管理するネットワーク内にいるものと認識する。したがって、データパケット暗号化ゲートウェイ４ａは、この計算機２と外部ネットワークを介したネットワーク１ｃ（図１参照）にいる計算機との間で通信されるパケットを転送する場合、図５の場合と同様の処理がなされる。

【００６８】次に、本発明の他の実施形態について説明する。図７は、本発明の他の実施形態に係る通信システムの構成を示す図である。図７（ａ）に示すように、経路間でデータパケットを暗号化するセキュリティルータ７１，７２，７３によりパケット転送経路が形成されている。経路上を通るデータパケットの暗号方式は、各ルータのペア間のネゴシエーションで決定され、各ルータのパラメータテーブル８０に格納されるものとする。

【００６９】ルータ７１により送信された暗号化パケットを経路途中のルータ７２が受信すると、ルータ７２は、パラメータテーブル８０を調べ、ルータ７１・ルータ７２間のデータパケット暗号化方式と、ルータ７２・ルータ７３間のデータパケット暗号化方式とが同じものであるか否かを調べる。

【００７０】両暗号化方式が同じであれば、ルータ７２は、パケット処理鍵Ｋｐのみをルータ７１・ルータ７２間の鍵暗号化方式で復号し、ルータ７２・ルータ７３間の鍵暗号化方式で再暗号化して、ルータ７３に転送する。

【００７１】これによって、データパケット全体の復号／再暗号化処理を回避することができる。ただし、ルータ７１・ルータ７２間のデータパケット暗号化方式と、ルータ７２・ルータ７３間のデータパケット暗号化方式とが異なるものである場合（すなわち、ルータ７１の暗号化方式をルータ７３で解読できない場合）は、図７（ｂ）に示すように、データ部の復号・暗号化など、データパケット全体を処理し直すことが必要である。

【００７２】なお、ここでは、ルータ３台の場合を示したが、パケット発信元（ルータ７１）の選択したパケット暗号化方式を転送経路のルータ群が処理できるならば、本発明に係るパケット処理鍵Ｋｐのみを復号／再暗号化する処理方法が適用できる。

【００７３】また、図１などを用いて説明した実施形態において、例えば、データパケット暗号化ゲートウェイ

４ｃとデータパケット暗号化ゲートウェイ４ａとの間に、図７のセキュリティルータが介在し、データパケット暗号化ゲートウェイ４ｃとセキュリティルータとの間、およびセキュリティルータとデータパケット暗号化ゲートウェイ４ａとの間で、それぞれ暗号通信を行うような場合にも、本発明に係るパケット処理鍵のみを復号／再暗号化する処理方法が適用できる。

【００７４】以上の図１～図７を用いて説明した各実施形態において、暗号通信をサポートするゲートウェイや計算機の間に暗号通信をサポートしないルータが介在する場合にも本発明は適用可能である。例えば、図１において外部ネットワーク内に暗号通信をサポートしないルータが存在する場合、あるいは図７において暗号通信をサポートするセキュリティルータ７１とセキュリティルータ７２の間に暗号通信をサポートしないルータが介在する場合にも、本発明は適用可能である。

【００７５】（第２の実施の形態）まず、本実施形態を概略的に説明する。移動計算機へのカプセル化によるパケット転送とパケット暗号化によるセキュリティとをサポートする通信システムにおいては、システムの要請に応じて様々なシステム実現方法が考えられる。このため、カプセル化の処理とパケット暗号化の処理が任意の順序で実行されるようなシステムも存在し得る。言い換えると、パケットを受信する装置側では、カプセル化の処理とパケット暗号化の処理がどのような順序で実行されるかを予め知ることはできないケースが想定される。

【００７６】例えば、第１の実施の形態で説明したように、図１のようにゲートウェイ（４ａ）にホームエージェントの機能を一部付与し、あるいはゲートウェイ（４ａ）とホームエージェント（５）を一体化して、ゲートウェイでの復号／再暗号化を避ける機能を使用する場合、ゲートウェイ４ａでは、パケット内にエンコードされたパケット処理鍵をゲートウェイ４ａ～４ｃ間で共有されるマスター鍵で復号し、これをゲートウェイ４ａ～移動計算機２間の別のマスター鍵で再暗号化した後に、パケット全体を移動計算機の現在位置宛にカプセル化して転送する。

【００７７】すると、図１５のように上記機能を使用しない場合には、

ホームエージェントでカプセル化→ゲートウェイで暗号化

という順序で処理を行っていたのに対し、上記機能を使用する場合には、

マスター鍵のみ再暗号化→全体をカプセル化

という逆の処理順序になる。

【００７８】ある受信側の移動計算機からみて上記ゲートウェイが上記機能の使用の有無を半固定的または動的に切り替える場合、あるいはホームネットワーク側の構成が変化して上記機能を持たないゲートウェイと上記機能を持つゲートウェイとが交換される場合には、または



システム構成要素間の位置関係に依っては、送信側でのパケットに対する移動処理および暗号化処理は任意の順序で行われるとともに、その順序は移動計算機側では予め（あるいは直ぐには）知ることができないので、受信する移動計算機側には送信側でどのような順序でパケット処理が行われていても正しく元のパケットを取り出すことのできる機能を持たせることが望ましい。

【００７９】このために本実施形態では、移動計算機内で、受信したパケットの最外側パケット形式を判別し、その判別結果に応じて移動計算機宛カプセル化を解く処理と暗号化パケットを復号する処理の実行順序を決定し、この実行順でパケット処理を行って、送信された元のパケットを復元する。

【００８０】これによって、移動計算機に対し、移動箇所アドレスのカプセル化処理と暗号化の処理を任意の順序で実行しても、移動計算機側で正しく内容を復元することができる。また、移動計算機システムの構成が容易に行え、またパケットの暗号化処理の最適化も行えるなど、システム性能の向上にも寄与できる。

【００８１】なお、移動計算機に対するパケットカプセル化形式は、例えば、ＩＥＴＦ　ＲＦＣ２００３に提案されるＩＰ－ｉｎ－ＩＰカプセル化や、ＲＦＣ２００４に提案されるＭｉｎｉｎｍａｌ　ｅｎｃａｐｓｕｌａｔｉｏｎを使用することができる。パケット暗号化形式は、例えばＲＦＣ１８２５－１８２７に提案されるＡｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｈｅａｄｅｒ（ＡＨ）とＥｎｃａｐｓｕｌａｔｅｄＳｅｃｕｒｉｔｙ　Ｐａｙｌｏａｄ（ＥＳＰ）およびＳＫＩＰ鍵管理方式（文献「ＳＫＩＰ：Ｓｉｍｐｌｅ　Ｋｅｙ－Ｍａｎａｇｅｍｅｎｔ　ｆｏｒ　Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ」，ＩＮＥＴ´９５等）の組合せ方式を使用することができる。

【００８２】パケットの最外側パケット形式の判別の基となる情報としては、例えばヘッダ内に記述される上記方式等で定義されたプロトコル型（プロトコルタイプ）を使用することができる。

【００８３】以下、本実施形態について詳しく説明する。図１５のような基本構成を持つネットワークを例にとる。図１５では、ホームネットワーク１ａ、外部のネットワーク１ｂ、外部のネットワーク１ｃがインターネット６を介して相互に接続されてる。ネットワーク１ａ，１ｃにはそれらが管理する計算機間で暗号化通信を行うためのデータパケット暗号化ゲートウェイ４ａ，４ｃが設置されている。移動計算機２もデータパケット暗号化ゲートウェイと同様のパケット暗号化機能を持つとする。これらのデータパケット暗号化ゲートウェイと移動計算機２の間での暗号化通信を行う。

【００８４】ここでは、ホームネットワーク１ａの移動計算機２が、移動の結果、ネットワーク１ｂにあり、移動計算機２がネットワーク１ｃにある通信相手ホスト３と暗号化通信する場合を考える。

19

【００８５】移動計算機２の位置情報の管理、移動計算機宛のパケットのルーティングを司るのがホームネットワーク内のホームエージェント（ＨＡ）５である。移動計算機がホームネットワークを離れ移動先に行くと、その位置情報を示す登録メッセージをホームエージェント５に送る。ホームエージェント５は、この情報を元に、移動計算機２宛のデータパケットがホームネットワークに到達したら、これを受け取って、パケット全体を、移動情報に示される現在位置を送信先とするデータパケットに成形（カプセル化）して、送信する。

【００８６】例えば、ＲＦＣ２００３ではＩＰパケットのペイロード部に元のホームアドレス宛パケットを埋め込んだＩＰ－ｉｎ－ＩＰ形式のカプセル化が規定されている。移動計算機はこのデータを受け取るとカプセル化を解いて所定のデータを受信する。

【００８７】この移動通信の規約に従って通信を行うと、図１５では、データパケット暗号化ゲートウェイ４ｃ～４ａ間で暗号通信が行われ、ゲートウェイ４ａで一旦復号されたデータがホームエージェント５に到達し、ホームエージェント５でカプセル化され、再度ゲートウェイ４ａで暗号かされる。そして、データパケット暗号化ゲートウェイ４ａ～移動計算機２間で再度暗号通信を行うことになる。移動計算機２は自身で暗号化パケットを復号し移動計算機宛のカプセル化パケットをデカプセル化することになる。この機能はＲＦＣ２００２にＣｏ－ｌｏｃａｔｅｄＣａｒｅ－ｏｆ　ａｄｄｒｅｓｓとして規定されている。

【００８８】図８に上記の方式で移動暗号化通信を行うパケット形式の一例を示す。パケットは通常のＩＰパケットヘッダの後に鍵情報ヘッダ、認証ヘッダ、暗号化ヘッダが続き、その後に暗号化されたデータ部が続く。

【００８９】上記のシステム構成では、ホームエージェント５で移動計算機２宛のカプセル化処理が施された後で、ゲートウェイ４ａで暗号化される。従って、暗号化されたデータ部は、移動計算機宛のＩＰ－ｉｎ－ＩＰカプセル化されたＩＰパケットからなる（図８の移動カプセル化部）。すなわち、ＩＰ－ｉｎ－ＩＰ形式の内部パケットを暗号化したパケットがインターネット上を流れ、移動計算機２はこれを受けて処理することになる。

【００９０】なお、図８において、ＩＰｖ４ヘッダの宛先は移動計算機ＭＮの現在位置アドレス、送信元はゲートウェイ４ａのグローバルアドレス、外側ＩＰヘッダの宛先は移動計算機ＭＮの現在位置アドレス、送信元はホームエージェントＨＡのグローバスアドレス、内側ＩＰヘッダの宛先は移動計算機ＭＮのホームアドレス、送信元は通信相手ＣＨのホームアドレスとする。

【００９１】さて、システム要求によっては、図１５のホームエージェント５と暗号化ゲートウェイ４ａを一体化すること、あるいは暗号化ゲートウェイ４ａにホームエージェント５の機能を一部搭載することが考えられる。後者は第１の実施の形態で既に説明したので前者について説明する。

20

【００９２】ホームエージェント５と暗号化ゲートウェイ４ａを一体化した場合、例えば暗号化ゲートウェイ４ａでの復号→ホームエージェントでの処理→再暗号化という２度の暗号処理を省く最適化が可能である。パケット内の鍵情報ヘッダには、鍵暗号化、パケット暗号化、認証のアルゴリズムの指定に加え、パケット処理鍵Ｋｐを２つのゲートウェイ間で共有されるマスター鍵ｋｉｊで暗号化したものをエンコードしてある。パケット処理鍵Ｋｐは送り手の側でランダムに生成される鍵で、これをもとにパケット認証鍵Ａ＿Ｋｐやパケット暗号化鍵Ｅ＿Ｋｐが計算される。ここで、パケット処理鍵Ｋｐが同じものであれば、暗号化通信のｅｎｄ－ｎｏｄｅが変更されても、暗号化されたデータ部や認証コードを変更する必要はなく、ｅｎｄ－ｎｏｄｅが変更された結果としてマスター鍵Ｋｉｊだけが変更されるので、このパケット形式の鍵情報ヘッダ部の「パケット鍵Ｋｐをマスター鍵Ｋｉｊで暗号化したもの」の部分のみを復号して再暗号化すればよい。この方針に従って、ホームエージェント５をゲートウェイ４ａに一体化して処理する実施形態を図９に示す（フォーリンエージェントは使用しないものと仮定する）。

【００９３】図９では、ホームネットワークのデータパケット暗号化ゲートウェイ４ａでパケット処理鍵Ｋｐの復号、およびゲートウェイ４ａ～移動計算機２間のマスター鍵での再暗号化に加え、本来ホームエージェントで行われていた、移動計算機２に対するデータのカプセル化処理も行うことが必要である。ホームネットワークのデータパケット暗号化ゲートウェイ４ａは、移動計算機２のホームアドレス宛のデータを受け取ると、ゲートウェイ４ａ～４ｃ間のマスター鍵で暗号化されているパケット処理鍵Ｋｐを復号し、ゲートウェイ４ａ～移動計算機２間のマスター鍵で再度暗号化する。さらに、移動情報を使い、移動計算機２の現在位置アドレスをヘッダとしてデータグラムをカプセル化して送信する。すなわち、パケット形式は図１０に示すように、外側が移動カプセル化形式で、内側が暗号化形式になる。

【００９４】なお、図１０において、ＩＰｖ４ヘッダの宛先は移動計算機ＭＮの現在位置アドレス、送信元はゲートウェイ４ａのグローバルアドレス、外側ＩＰヘッダの宛先は移動計算機ＭＮの現在位置アドレス、送信元はホームエージェントを兼ねているゲートウェイ４ａのグローバスアドレス、内側ＩＰヘッダの宛先は移動計算機ＭＮのホームアドレス、送信元は通信相手ＣＨのホームアドレスとする。

【００９５】これを受信した移動計算機２は、まず外側の形式が移動カプセル化であることを判別しデカプセル化処理を行い、次に内側の暗号化処理を行う。すなわち、図１５のシステムとは逆の順序でパケットを処理す

ーリンエージェント７はこれを受けて処理することになる。

【０１０２】しかし図１２においても、送信側でカプセル化の処理とパケット暗号化の処理の順序が任意に行われる場合には、前述した移動計算機の場合と同様に、パケット転送を行うフォーリンエージェントには送信側でどのような順序でパケット処理が行われていても転送処理を行うことのできる機能を持たせることが望ましい。

【０１０３】また、システム要求によっては、図１２のフォーリンエージェント７と暗号化ゲートウェイ４ｂを一体化することが考えられる。これを図１３に示す。この場合も上記と同様に、送信側でカプセル化の処理とパケット暗号化の処理の順序が任意に行われるならば、パケット転送を行うフォーリンエージェント機能を有するデータパケット暗号化ゲートウェイには送信側でどのような順序でパケット処理が行われていても転送処理を行うことのできる機能を持たせることが望ましい。

【０１０４】図１４に、移動計算宛カプセル化とパケット暗号化のサポートされたパケット転送を行うフォーリンエージェントまたはフォーリンエージェント機能を有するデータパケット暗号化ゲートウェイが、移動計算機にパケットを転送するための手順の一例を示す。

【０１０５】まず、受信したパケットの最外側パケット形式を判別する（ステップＳ２１，Ｓ２２）。パケット形式の判別には、移動ＩＰ（ＲＦＣ２００３）やＩＰセキュリティ（ＲＦＣ１８２５など）で定義されている、ＩＰのプロトコル番号やｎｅｘｔ　ｐｒｏｔｏｃｏｌフィールドを使用することができる。例えば、ＩＰ－ｉｎ－ＩＰ形式はプロトコル番号４で識別でき、暗号パケットはＩＰヘッダのｎｅｘｔ－ｈｅａｄｅｒフィールドが特定の認証ヘッダ、暗号化ヘッダ識別コードであることで識別できる。

【０１０６】最外側パケット形式が移動計算機宛カプセル化形式であると判別された場合は、まず、カプセル化を解く処理を行う（ステップＳ２３）。そして、得られた暗号化パケットの宛先を調べ（ステップＳ２４）、宛先が自装置の場合は復号処理を行い（ステップＳ２５）、自装置内に取り込んで（ステップＳ２６）、他の必要な処理を行う。もし宛先が移動計算機２の場合は、暗号パケットを転送する（ステップＳ２７）。

【０１０７】一方、最外側パケット形式が暗号化パケット形式であると判別された場合は、外側の暗号パケットの宛先を調べ（ステップＳ２８）、宛先が自装置である場合は、復号処理を行い（ステップＳ２９）、さらに中の移動カプセル化パケットの処理も行う（ステップＳ３０）。外側の暗号パケットの宛先が移動計算機２の場合は、そのままパケット全体を転送する（ステップＳ２７）。

【０１０８】なお、この場合、移動計算機は、まず復号を行い、得られたパケットがカプセル化されたものであ

ｶﾌﾟｾﾙ化とﾊﾟｹｯ
通信を行う移動計算
り出すための手順の

ｯﾄの最外側ﾊﾟｹｯﾄ
、Ｓ１２）。ﾊﾟｹｯﾄ
Ｃ２００３）やＩＰｾ
ﾀﾞ）で定義されている、
ｔ　ｐｒｏｔｏｃｏｌﾌ
る。例えば、ＩＰ－ｉｎ
で識別でき、暗号ﾊﾟｹｯ
ｈｅａｄｅｒﾌｨｰﾙﾄﾞが
ｯﾀﾞ識別ｺｰﾄﾞであること

形式が移動計算機宛ｶﾌﾟｾ
場合は、先にｶﾌﾟｾﾙ化を
Ｓ１３）、得られた暗号化ﾊﾟ
う（ｽﾃｯﾌﾟＳ１４）。一
暗号化ﾊﾟｹｯﾄ形式であると
号化ﾊﾟｹｯﾄを復号する処理
、得られた移動計算機宛ｶﾌﾟ
ﾙ化を解く処理を行う（ｽﾃｯ

移動計算機について説明したが、
ｰﾄｳｪｲについて説明する。図
を持つﾈｯﾄﾜｰｸを例にとる。
５の構成において、移動計算機２
ｰｸ内に、移動してきた計算機への
ﾌｫｰﾘﾝｴｰｼﾞｪﾝﾄ７を配置し
ｰﾘﾝｴｰｼﾞｪﾝﾄ７はＲＦＣ２０
のを用いるものとする。
では、移動計算機２は暗号ﾊﾟｹｯﾄの
ｫｰﾘﾝｴｰｼﾞｪﾝﾄ７は移動計算機
理を担当するとする。この場合、ﾎｰ
処理されたＩＰ－ｉｎ－ＩＰﾊﾟｹｯﾄ
ａで処理されて（ＩＰｓｅｃ－ｉｎ－
ﾌｫｰﾘﾝｴｰｼﾞｪﾝﾄ７に到達する。ﾌ
ｪﾝﾄは最初にﾃﾞｶﾌﾟｾﾙ化を行い、次
理されたﾊﾟｹｯﾄが移動計算機２に渡さ
画される。
図１２のﾌｫｰﾘﾝｴｰｼﾞｪﾝﾄ７を持つ
では、ｹﾞｰﾄｳｪｲ４ａとﾌｫｰﾘﾝｴｰ
の間を流れるﾊﾟｹｯﾄは、図１０のような
このﾊﾟｹｯﾄは外側が移動ＩＰでｶﾌﾟｾﾙ
Ｐ－ｉｎ－ＩＰ形式で、内側ＩＰﾊﾟｹｯﾄが
ﾄﾍｯﾀﾞの後に鍵情報ﾍｯﾀﾞ、認証ﾍｯﾀﾞ、
ﾀﾞが続く暗号化形式になっている。すなわ
化形式の内部ﾊﾟｹｯﾄをＩＰ－ｉｎ－ＩＰでｶ
したﾊﾟｹｯﾄがｲﾝﾀｰﾈｯﾄ上を流れ、ﾌｫ

れば、これをデカプセル化する。ところで、各ネットワークのポリシー等によっては、図１２のフォーリンエージェント７～移動計算機２間や図１３のゲートウェイ４ｂ～移動計算機２間を暗号化しない平文パケットを転送してもよい場合がある。このような場合には、図１２のフォーリンエージェント７や図１３のゲートウェイ４ｂが移動計算機ＭＮに代って暗号パケットの復号処理まで行うことも考えられる。

【０１０９】この場合の手順は図１１と同様である。なお、以上の各機能は、ソフトウェアとしても実現可能である。また、上記した各手順あるいは手段をコンピュータに実行させるためのプログラムを記録した機械読取り可能な媒体として実施することもできる。

【０１１０】また、本発明は、ＲＦＣ２００２～２００４およびＲＦＣ１８２５～１８２９に示される移動ＩＰおよびＩＰセキュリティプロトコルだけでなく、他の様々な移動通信プロトコル、暗号化通信プロトコル、暗号鍵交換プロトコルに対しても適用可能である。本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【０１１１】

【発明の効果】本発明によれば、パケット処理装置において、転送されてきた暗号化パケットのデータ部に対する所定の処理は行わずに、パケット処理鍵のみ復号・再暗号化して宛先計算機へ向けて転送することにより、全てのパケットについてデータ部に対する所定の処理を行う従来技術と比べ、パケット処理のオーバーヘッドを低減することができる。

【０１１２】また、本発明によれば、パケット処理装置において、自装置の管理するネットワーク外の計算機宛のパケットであれば、パケット処理鍵のみ復号・再暗号化して宛先計算機へ向けて転送することにより、全てのパケットについてデータ部に対する所定の処理を行う従来技術と比べ、パケット処理のオーバーヘッドを低減することができる。

【０１１３】また、本発明によれば、移動計算機へのカプセル化によるパケット転送とパケット暗号化によるセキュリティ対応をシステム構成要素間の位置関係やパケット処理の最適化などのシステム側の要求のため送信側で任意の順序で行っても、受信する移動計算機側で受信したパケットの最外側パケットの形式を判別しその判別結果に応じて移動計算機宛カプセル化を解く処理と暗号化パケットを復号する処理を必要な順序で施して、送信



された元のパケットを復元することができる。これにより、移動計算機システムの構成が容易に行え、またパケットの暗号化処理の最適化も行えるなど、システム性能の向上にも寄与できる。

【図面の簡単な説明】

【図１】本発明の一実施形態に係るネットワーク構成を示す図

【図２】本発明の一実施形態に係るデータパケット形式の一例を示す図

【図３】本発明の一実施形態に係る各ノードでのデータパケット処理の流れを示す図

【図４】通信相手がホームネット内にある場合を示す図

【図５】移動計算機がホームネット内にある場合を示す図

【図６】階層構造を持つネットワークの一例を示す図

【図７】本発明の他の実施形態に係るシステム構成を示す図

【図８】データパケット形式の一例を示す図

【図９】本発明のさらに他の実施形態に係るネットワーク構成を示す図

【図１０】データパケット形式の一例を示す図

【図１１】移動計算機の手順の一例を示すフローチャート

【図１２】本発明のさらに他の実施形態に係るネットワーク構成を示す図

【図１３】本発明のさらに他の実施形態に係るネットワーク構成を示す図

【図１４】フォーリンエージェントおよびフォーリンエージェント機能を有するデータパケット暗号化ゲートウェイの手順の一例を示すフローチャート

【図１５】暗号通信を伴う移動通信をサポートする通信システムの基本構成を説明するための図

【符号の説明】

１ａ，１ｂ，１ｃ…ネットワーク

２，２２，３２…移動計算機

３…通信相手

４ａ，４ｃ，４ｂ，４ｅ…ゲートウェイ

５…ホームエージェント

６…インターネット

７…フォーリンエージェント

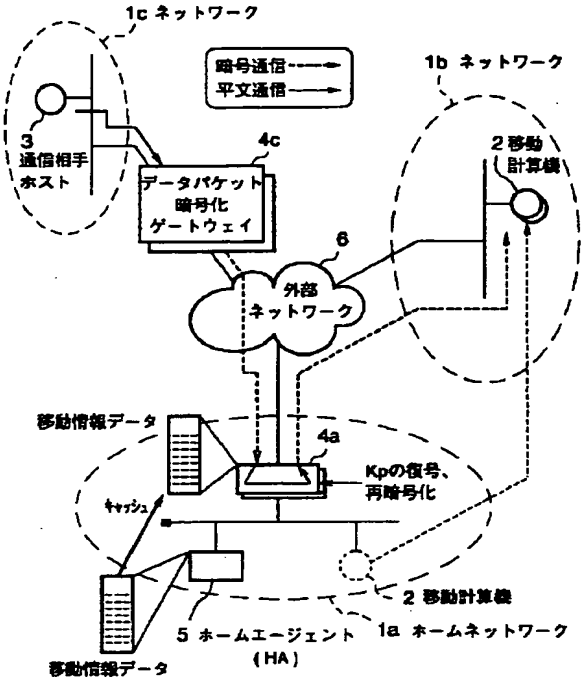
１４ｆ…ルータ

２１，２２，２３…バス

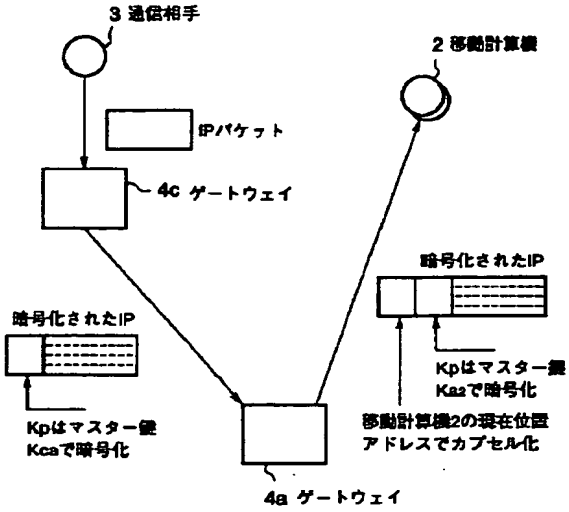
７１，７２，７３…セキュリティルータ

８０…パラメータテーブル

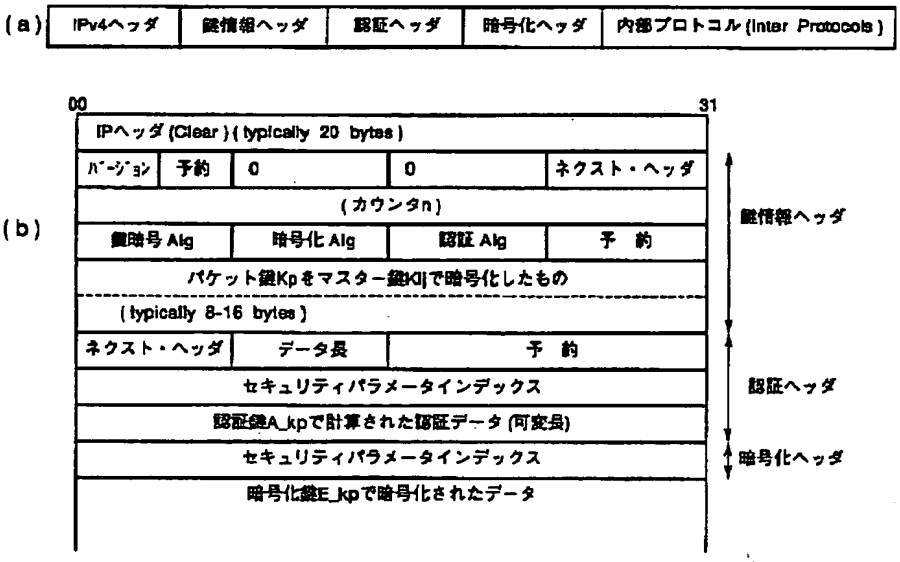
【図１】


1c ネットワーク
暗号通信
平文通信
1b ネットワーク
3
通信相手
ホスト
4c
データパケット
暗号化
ゲートウェイ
2 移動
計算機
6
外部
ネットワーク
移動情報データ
4a
Kpの復号、
再暗号化
キャッシュ
2 移動計算機
5 ホームエージェント
(HA)
1a ホームネットワーク
移動情報データ

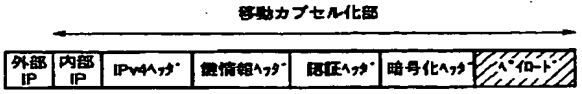
【図３】


3 通信相手
2 移動計算機
IPパケット
4c ゲートウェイ
暗号化されたIP
暗号化されたIP
Kpはマスター鍵
Kaaで暗号化
Kpはマスター鍵
Kcaで暗号化
移動計算機2の現在位置
アドレスでカプセル化
4a ゲートウェイ

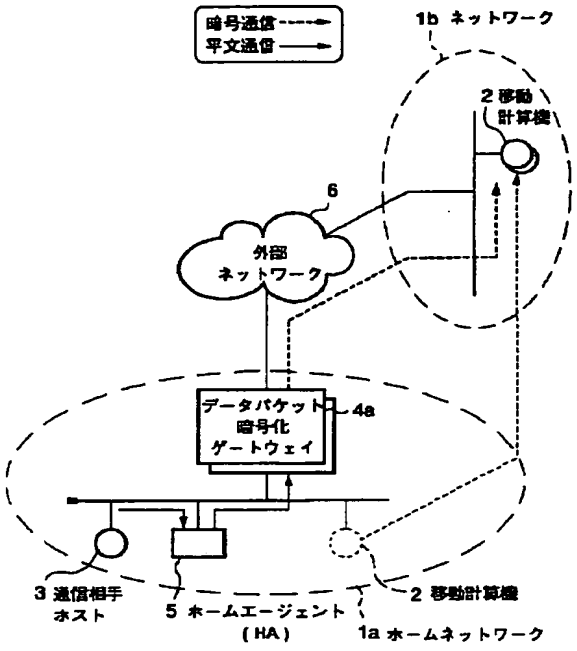
【図２】


(a)
IPv4ヘッダ
鍵情報ヘッダ
認証ヘッダ
暗号化ヘッダ
内部プロトコル (Inter Protocols)
(b)
00
31
IPヘッダ (Clear) ( typically 20 bytes )
バージョン
予約
0
0
ネクスト・ヘッダ
(カウンタn)
鍵暗号 Alg
暗号化 Alg
認証 Alg
予 約
パケット鍵Kpをマスター鍵Kjで暗号化したもの
( typically 8-16 bytes )
ネクスト・ヘッダ
データ長
予 約
セキュリティパラメータインデックス
認証鍵A_kpで計算された認証データ (可変長)
セキュリティパラメータインデックス
暗号化鍵E_kpで暗号化されたデータ
鍵情報ヘッダ
認証ヘッダ
暗号化ヘッダ

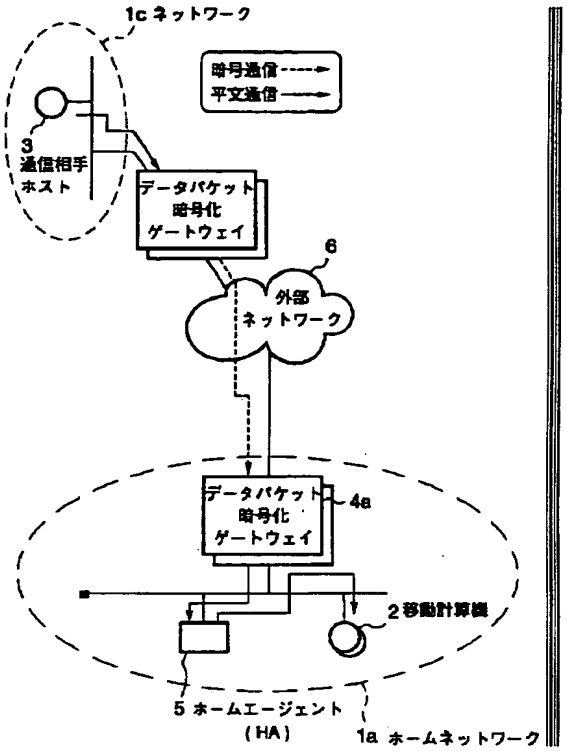
【図１０】


移動カプセル化部
外部 IP
内部 IP
IPv4ﾍｯﾀﾞ
鍵情報ﾍｯﾀﾞ
認証ﾍｯﾀﾞ
暗号化ﾍｯﾀﾞ
ﾍﾟｲﾛｰﾄﾞ

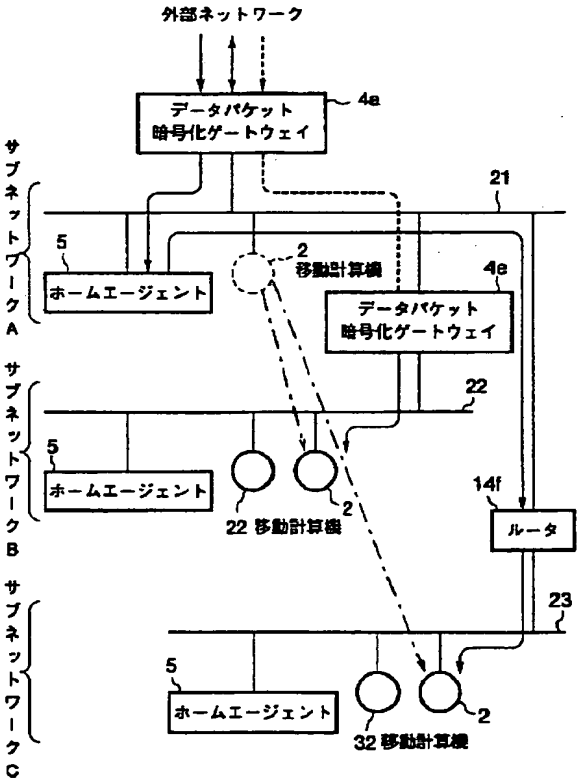
【図４】


暗号通信
平文通信
1b ネットワーク
2 移動計算機
6
外部ネットワーク
データパケット暗号化ゲートウェイ
4a
3 通信相手ホスト
5 ホームエージェント (HA)
2 移動計算機
1a ホームネットワーク

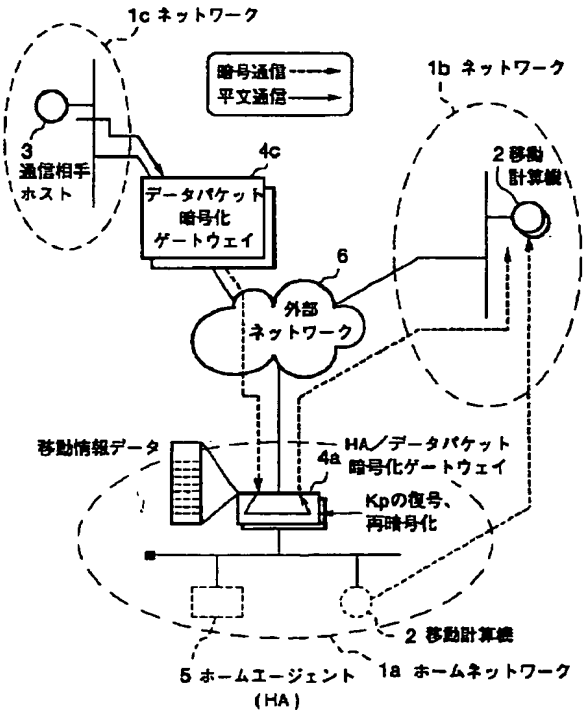
【図５】


1c ネットワーク
暗号通信
平文通信
3 通信相手ホスト
データパケット暗号化ゲートウェイ
6
外部ネットワーク
データパケット暗号化ゲートウェイ
4a
2 移動計算機
5 ホームエージェント (HA)
1a ホームネットワーク

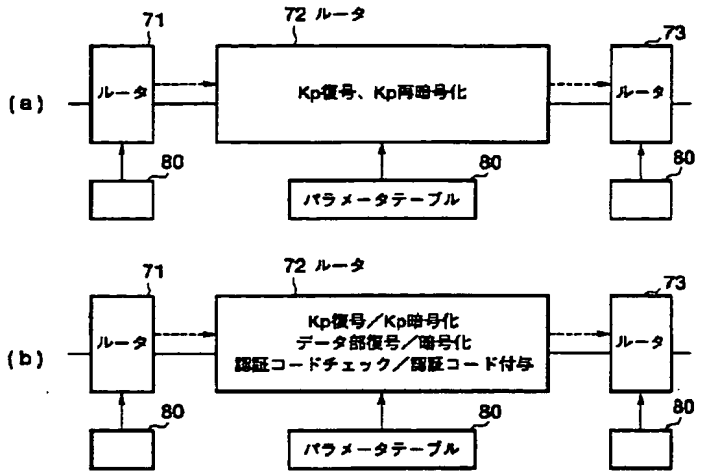
【図６】


外部ネットワーク
データパケット暗号化ゲートウェイ
4a
21
サブネットワークA
5
ホームエージェント
2 移動計算機
4e
データパケット暗号化ゲートウェイ
22
サブネットワークB
5
ホームエージェント
22 移動計算機
2
14f
ルータ
23
サブネットワークC
5
ホームエージェント
32 移動計算機
2

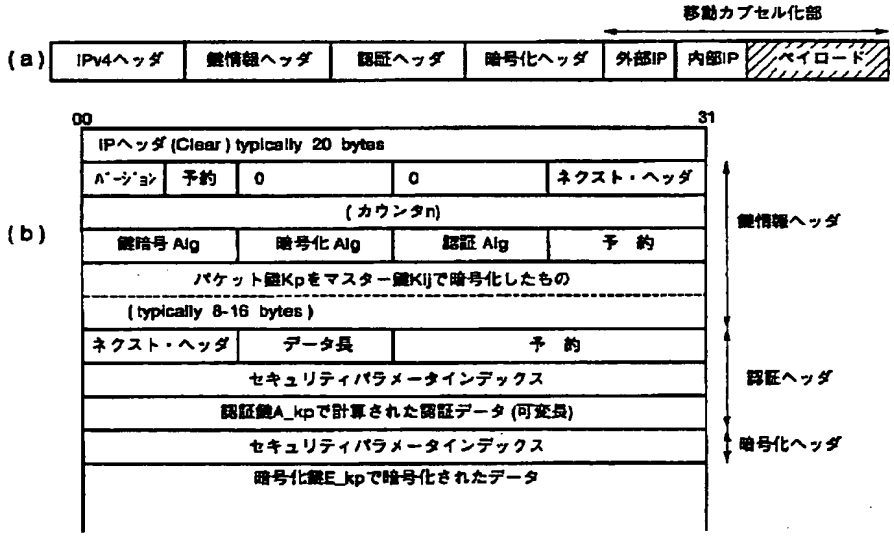
【図９】


1c ネットワーク
暗号通信
平文通信
1b ネットワーク
3 通信相手ホスト
4c
データパケット暗号化ゲートウェイ
2 移動計算機
6
外部ネットワーク
移動情報データ
HA／データパケット暗号化ゲートウェイ
4a
Kpの復号、再暗号化
2 移動計算機
5 ホームエージェント (HA)
1a ホームネットワーク

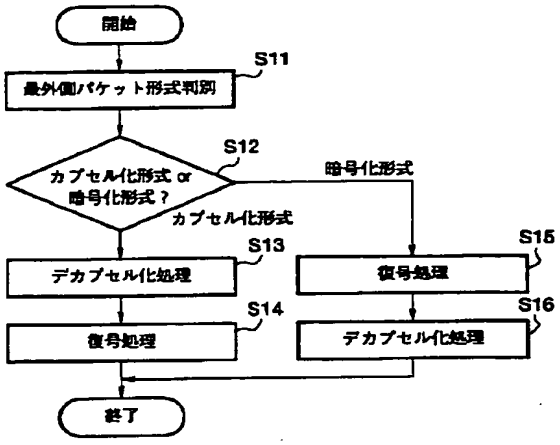
【図７】


(a)
71
72 ルータ
73
ルータ
Kp復号、Kp再暗号化
ルータ
80
80
80
パラメータテーブル
(b)
71
72 ルータ
73
ルータ
Kp復号／Kp暗号化
データ部復号／暗号化
認証コードチェック／認証コード付与
ルータ
80
80
80
パラメータテーブル

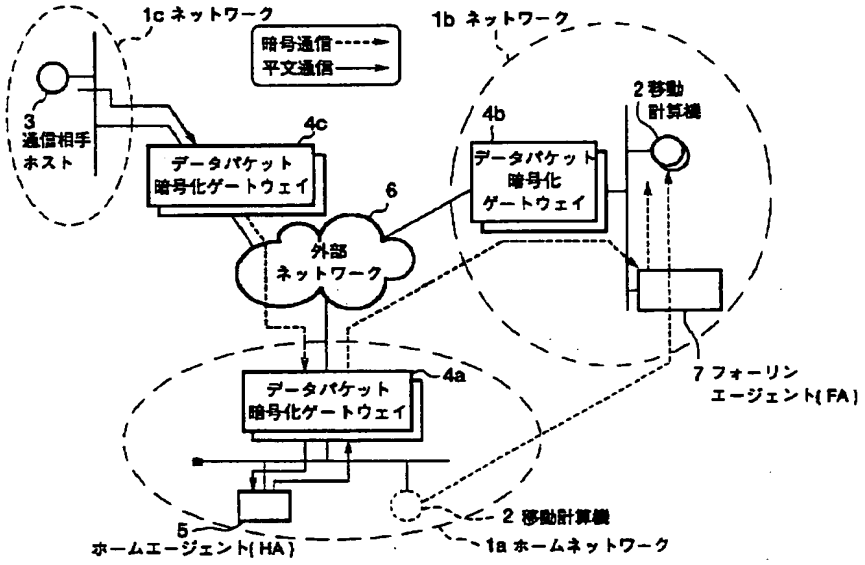
【図８】


移動カプセル化部
(a)
IPv4ヘッダ
鍵情報ヘッダ
認証ヘッダ
暗号化ヘッダ
外部IP
内部IP
ペイロード
(b)
00
31
IPヘッダ (Clear) typically 20 bytes
ﾊﾞｰｼﾞｮﾝ
予約
0
0
ネクスト・ヘッダ
(カウンタn)
鍵暗号 Alg
暗号化 Alg
認証 Alg
予 約
パケット鍵Kpをマスター鍵Kijで暗号化したもの
(typically 8-16 bytes)
ネクスト・ヘッダ
データ長
予 約
セキュリティパラメータインデックス
認証鍵A_kpで計算された認証データ (可変長)
セキュリティパラメータインデックス
暗号化鍵E_kpで暗号化されたデータ
鍵情報ヘッダ
認証ヘッダ
暗号化ヘッダ

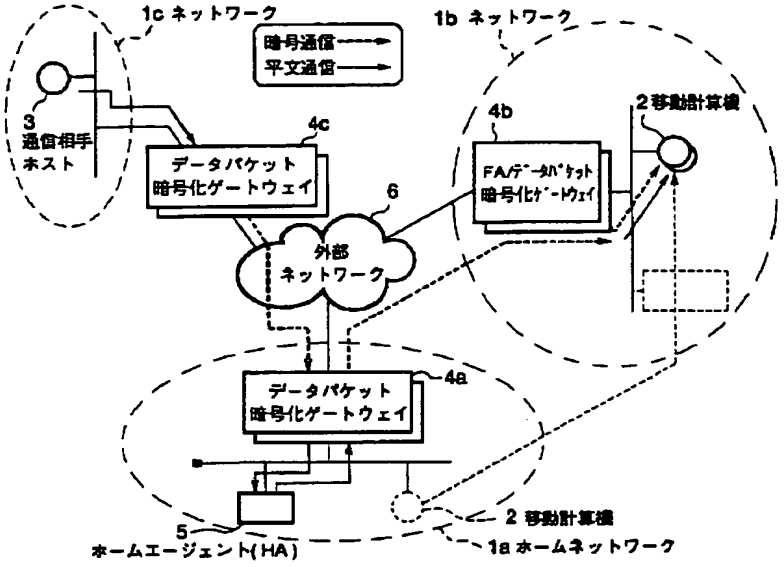
【図１１】


開始
S11
最外側パケット形式判別
S12
カプセル化形式 or
暗号化形式？
暗号化形式
カプセル化形式
S13
デカプセル化処理
S14
復号処理
S15
復号処理
S16
デカプセル化処理
終了

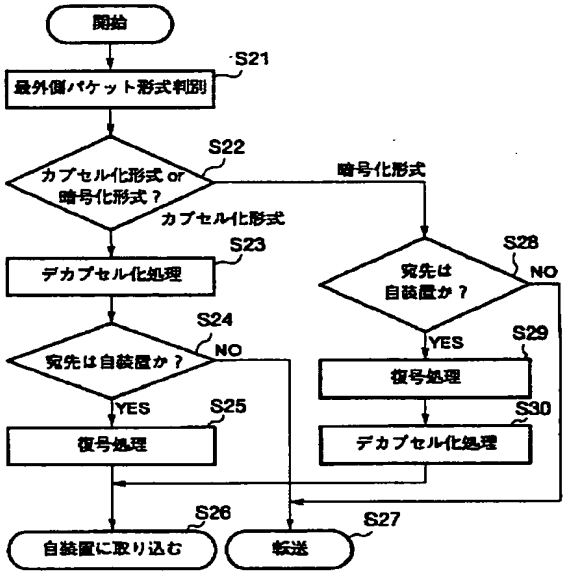
【図１２】


1c ネットワーク
暗号通信
平文通信
1b ネットワーク
3
通信相手
ホスト
4c
データパケット
暗号化ゲートウェイ
6
外部
ネットワーク
4b
データパケット
暗号化
ゲートウェイ
2 移動
計算機
4a
データパケット
暗号化ゲートウェイ
7 フォーリン
エージェント(FA)
5
ホームエージェント(HA)
2 移動計算機
1a ホームネットワーク

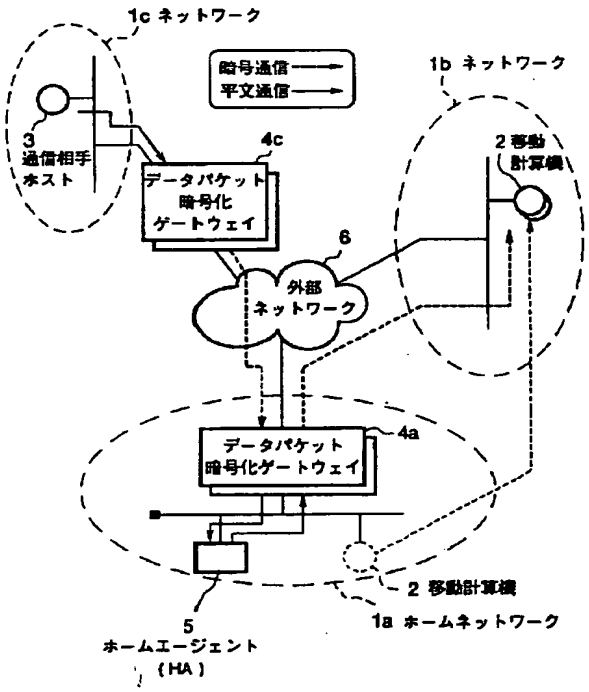
【図１３】


1c ネットワーク
暗号通信
平文通信
1b ネットワーク
3
通信相手
ホスト
4c
データパケット
暗号化ゲートウェイ
4b
FA/データパケット
暗号化ゲートウェイ
2 移動計算機
6
外部
ネットワーク
4a
データパケット
暗号化ゲートウェイ
5
ホームエージェント(HA)
2 移動計算機
1a ホームネットワーク

【図１４】


開始
S21
最外側パケット形式判別
S22
カプセル化形式 or
暗号化形式？
暗号化形式
カプセル化形式
S23
デカプセル化処理
S24
宛先は自装置か？
NO
YES
S25
復号処理
S26
自装置に取り込む
S28
宛先は
自装置か？
NO
YES
S29
復号処理
S30
デカプセル化処理
S27
転送

【図１５】


1c ネットワーク
暗号通信
平文通信
1b ネットワーク
3
通信相手
ホスト
4c
データパケット
暗号化
ゲートウェイ
2 移動
計算機
6
外部
ネットワーク
4a
データパケット
暗号化ゲートウェイ
2 移動計算機
1a ホームネットワーク
5
ホームエージェント
(HA)

フロントページの続き

(72)発明者　津田　悦幸
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(72)発明者　新保　淳
東京都府中市東芝町１番地　株式会社東芝府中工場内

(72)発明者　岡本　利夫
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内